DATA PROTECTION & VOICE ASSISTANTS

In this brAInfood, the Knowlegde Centre Data & Society provides more information on a number of privacy and data protection concerns related to the use of voice assistants.

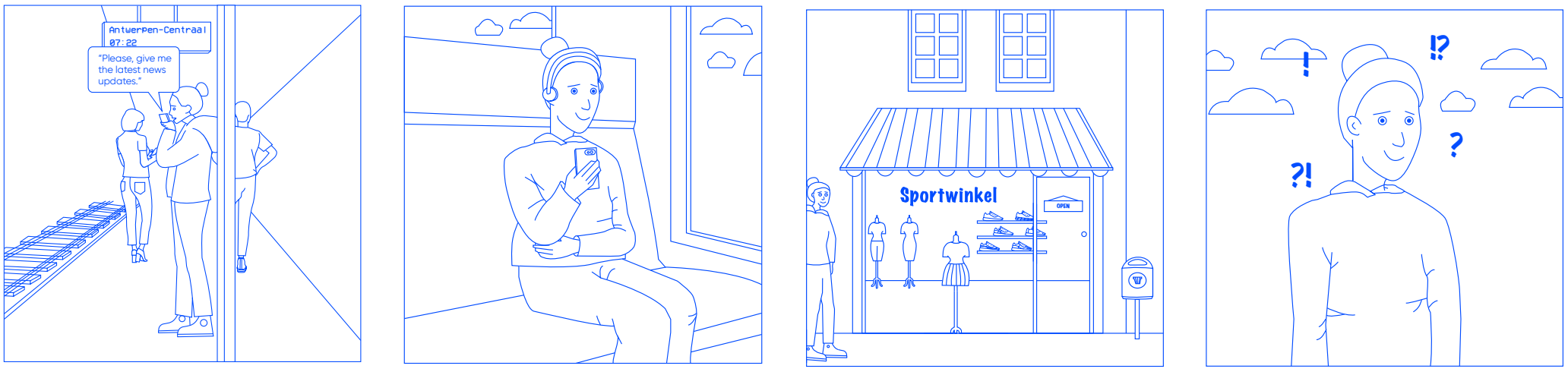
We illustrate these points of attention by means of a story in which Kate plays the main character. Read the story (see the right column) and the additional information that goes into more detail on a specific topic (transparency, data collection, privacy, security and data re-use) to learn more about the processing of data of voice assistants.

In the future, the Knowledge Centre Data & Society will investigate how other data applications and AI technologies deal with privacy and data protection. To be continued …

Kate has to attend a workshop in Antwerp for her work. She goes by train from Brussels and asks her voice assistant to give her an overview of the latest news updates. She listens to these updates with her headphones so that she doesn't disturb others on the train.

Upon arrival in Antwerp-Central station, she asks her voice assistant to give her the quickest route to the location of the workshop. During the walk she notices that she often passes by sports stores.

On the train, just yet, she searched online for new sports shoes via her smartphone. She wonders 'Would this be the quickest route?'. She doubts whether her voice assistant intentionally has set out a route that leads her through the shopping street with its many sports stores.



Repurpose of data

The **sound recordings** that Kate makes through her voice assistant are not just used to answer her question. By analysing the collected data, it is possible for the manufacturer to know or deduce her interests, planning, driving routes or habits. This data can be used, without her knowledge, to **create a profile** and to **provide unsolicited personal services**, such as advertising or modified search results. Voice assistants use this data to provide the user with the best possible service.

Privacy

Kate presupposes that the questions she asks her voice assistant are recorded and handled by technology, without any **staff listening in to the audio fragments**. Until recently, however, this was done at various producers of voice assistants, without the users being informed. After these practices were criticised, the companies adapted their policies. One company has temporarily stopped the listening practices, while others are asking for the approval of their users. Kate may therefore want to consult the **privacy policy** of her voice assistant.

Collecting data

Online shopping and passing sports shops on her way to the workshop got Kate thinking. It is not clear to her how long the assistant stores the recordings. She realises that her voice assistant posseses a lot of personal information, and is considering removing her **recording history**.

In most cases, the companies behind virtual assistants leave the **initiative to delete data to users**. In some cases, it is not even possible to delete all the stored data. Depending on the virtual assistant, the delete function may only partially delete the data, for example only voice data.

Transparency

Like many other users, Kate has not fully reviewed the **privacy statement** of her voice assistant. Kate saw the statement when she installed the assistant, but she did not go through the text in detail. She does not realise, therefore, that when she agreed to the privacy statement, her voice recordings can also be used to derive her health status and emotional state.

Security

Kate's virtual assistant not only collects her data via her voice recordings. The voice assistant can **also collect data from other devices linked to the assistant**. Kate has connected her voice assistant to other smart applications, such as her robot vacuum cleaner. The combination of all this data from all these different applications results in a large amount of data. This data is very personal and can lead to impressive results that can be interesting for Kate. But the downside of this story is that this large amount of data can also be very attractive to hackers.